RESPONSES TO THE EUROPEAN DATA PROTECTION BOARD'S CONSULTATION REGARDING RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

SPEED READ

EMW welcomes the opportunity to contribute formally to this consultation.

The draft guidance lacks realistic and pragmatic help for businesses unable to command the attention of the (mainly US-based) giants of the IT ecosystem. It creates more questions than answers. The draft recommendation seems almost unable to acknowledge that several countries (the US in particular) hold a monopoly in IT software and service provision. Some, perhaps most, of the entities in those territories are unable to avoid the reach of surveillance duties hardwired into their national law. Indeed, imposing some of the recommendations of the draft guidance may put those entities in breach of their national laws. This draft guidance should take into account the international contours of the IT ecosystem and speak more plainly to businesses unable to negotiation technical or contractual changes and equally unable to buy services from elsewhere due the aforementioned monopoly.

- **Step 3: Assessing the level of protection in third countries** We ask the EDPB to focus on requiring a proportionate level of analysis based on a risk-based assessment.

- **Step 4: Supplementary Measures**. We ask the EDPB to give more consideration to other supplementary measures and where technological measures are recommended clarify and give a realistic standards.

- **Step 6: Re-evaluate at appropriate intervals** Further guidance is required, particularly to determine what constitutes an 'appropriate interval' and what are the triggers for a re-evaluation to take place.

INTRODUCTION

This document sets out EMW's response to the European Data Protection Board (EDPB) recommendations[1] regarding measures to supplement transfer tools to ensure compliance with the EU protection of personal data ("**Draft Recommendations**"). It is EMW's view that the recommendations reinforce much of the existing principles of the GDPR, which includes the continuing obligation of accountability. However they appear to set a course away from a risk based approach, especially when data exporters are required to assess the adequacy of a third country's data protection laws and what supplementary measures would adequately protect the data subject's interests.

The Draft Recommendations place a disproportionate burden onto data exporters by requiring them to assess whether the laws to which a third party is subject are incompatible with the fundamental rights and freedoms enshrined in the GDPR. This is a daunting task for many UK businesses. For some it is simply an unrealistic, unattainable burden. It lacks realistic and pragmatic help for businesses unable to command the attention of the (mainly US-based) giants of the IT ecosystem. The draft recommendation seems almost unable to acknowledge that several countries (the US in particular) hold a monopoly in IT software and service provision.

Our consultation response sets out detailed explanations regarding each of the points that we have identified, but in summary:

- **Step 3: Assessing the level of protection in third countries** The requirements at Step 3 go beyond what was envisaged by the GDPR and put unnecessary and disproportionate obligations on data exporters to assess the level of protection in third countries. We call on the EDPB to instead focus on requiring a proportionate level of analysis based on a risk-analysis and how this will inform the supplementary measures that data exporters can take.

- **Step 4: Supplementary Measures** Step 4 focuses too heavily on technological measures, which are unclear and also unrealistic in light of the IT ecosystem and its US-leaning bias. We call on the EDPB to instead give more consideration to other supplementary measures and where technological measures are recommended clarify and give a realistic standard.

- **Step 5: Taking procedural steps if the supplementary measures are proven effective** Further information is required concerning the implications of the Schrems II judgment concerning Binding Corporate Rules and ad hoc contractual clauses. This section is therefore incomplete.

- **Step 6: Re-evaluate at appropriate intervals** Further guidance is required, particularly to determine what constitutes an 'appropriate interval' and what are the triggers for a re-evaluation to take place. The uncertainties in the previous steps, particularly steps 3 and 4, are reinforced in step 6 which ultimately requires the data exporter to repeat a process which was from the start vague and full of uncertainty.

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data referred to throughout as "the **Draft Recommendations**"

DETAILED RESPONSES

Issue 1: Step 3 - Assessing the level of protection in third countries

Your Draft Recommendations
The Draft Recommendations say: *"…Therefore, you must assess, where appropriate in collaboration with the importer, if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer. Where appropriate, your data importer should provide you with the relevant sources and information relating to the third country in which it is established and the laws applicable to the transfer. You may also refer to other sources of information, such as the ones listed non-exhaustively in Annex 3…* *…You should in any case pay specific attention to any relevant laws, in particular laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision and national security purposes). If these requirements or powers are limited to what is necessary and proportionate in a democratic society,42 they may not impinge on the commitments contained in the Article 46 GDPR transfer tool you are relying on…* *… In carrying out this assessment, different aspects of the legal system of that third country, e.g. the elements listed in Article 45(2) GDPR, are also be relevant.43 For example, the rule of law situation in a third country may be relevant to assess the effectiveness of available mechanisms for individuals to obtain (judicial) redress against unlawful government access to personal data. The existence of a comprehensive data protection law or an independent data protection authority, as well as adherence to international instruments providing for data protection safeguards, may contribute to ensuring the proportionality of government interference.44…* *…Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors45…"*[2]
Our Response
It is our view that the paragraphs above and the wider "Step 3" recommendations are interpretative overreaching on the part of the EDPB. Whilst in case C-311/18 the Court came to the conclusion that, when relying on Article 46 of the GDPR, the requirement that enforceable data subject rights and effective legal

[2] Draft Recommendations, pages 12-14

remedies for data subjects be an available means that an assessment corresponding to the factors listed in Article 45(2) is required, the EDPB Draft Recommendations go beyond this.

Lack of Legal Evidence

Article 45 of the GDPR and Recitals 103-107 specifically refer to only the Commission. Despite the Court's judgement in case C-311/18, the wording of Article 45 and Recitals 103-107 makes clear that it was never envisaged that individual controllers and processors would be placed under the exact same (or even higher) obligations. The Court's judgement also only states that "the factors to be taken into consideration in the context of Article 46 of that regulation ***correspond*** (our emphasis added) to those set out, in a non-exhaustive manner, in Article 45(2)" and not that they exactly match them.

Practical Issues

The Commission, through the process of issuing and reviewing Adequacy Decisions, already considers the factors listed in Article 45 of the GDPR and as required by Article 45(8) to publish its decision as to whether an adequate level of protection is or is no longer ensured. The EDPB Draft Recommendations' requirement that data exporters wishing to use an Article 46 tool go through the exact same process, when the Commission has not issued an Adequacy Decision, and has twice conducted an exercise of assessment which ultimately floundered[3], is therefore unnecessary. Not only is it economically unviable (as rather than one analysis being conducted, tens-of-thousands are conducted), but it in essence suggests that individual data exporters can come to a different conclusion to the one the Commission reaches.

The Draft Recommendations refer to many different sources which a controller or processor may/can/should consider in addition to those that have to/must be considered. These go further than the factors to be considered under Article 45(2). There is also no guidance as to which sources take priority if for example some conflicted.

The Draft Recommendations suggest that the analysis can be carried out "*where appropriate in collaboration with the importer*". No guidance is however given as to when this is appropriate. Whilst in theory data exporters working in collaboration with data importers to complete the analysis could be a good way to reduce the cost of any analysis, we foresee multiple issues with this (even if the collaboration is limited to simply providing relevant sources and information). In particular: generally it will be in the data importer's interest for the transfer to go ahead (so bias, whether conscious or not, will likely play a part); it assumes that the data importer understands the EU data protection system; and if it does go wrong and the data exporter is hit with a data protection fine, whilst the data exporter could sue the importer, due to the size of data protection fines recovery is highly unlikely.

At paragraph 42 of the Draft Recommendations it states that "*you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards*". The "objective factors" referred to though includes – "*Elements demonstrating that a third country authority will seek to access the data…. will be able to access the data*". This appears somewhat contradictory and unclear.

Commercial Impact

The current Draft Recommendations' "Step 3" requirements will cause major commercial impact upon businesses. In order to comply it would require numerous experts and professional advisors to be

[3] We refer to the Safe Harbor decision 2000/520 and Privacy Shield decision 2016/1250

hired/engaged on an ongoing basis. The amount of time it would take to properly analyse a new or potential third country's legal system in line with the Draft Recommendations (The length of the Commission's own analysis and adequacy negotiations demonstrate this effectively) would also likely prevent opportunities from being seized.

The reality is that for many businesses these would simply not be feasible and so the resulting effect would likely either be cases of non-compliance with the Draft Recommendations or a reduction in world trade and competition. Any reasonable observer would recognise the benefits of enhanced competition and compliance. The practical effect of the Draft Recommendations is that not only are would-be data exporter interests hindered by unnecessarily burdensome rules promulgated by the EDPB, but so are the data subjects' interests.

Conclusion For Issue 1

In our view, the Court's decision in Case C-311/18 has been misinterpreted by the EDPB and resulted in the Draft Recommendations overreaching and adding unnecessary obligations on data exporters to the detriment of all. The Draft Recommendations' extensive analysis requirements at Step 3 are causing significant commercial concern. In our opinion, the recommendations should instead focus on a proportionate level of analysis based instead on a risk-analysis and how this will inform the supplementary measures that data exporters can take and we ask EDPB to therefore reconsider its recommendations before its final version is published.

Issue 2: Step 4 - Unrealistic Supplementary Measures which are not proportional

Your Draft Recommendations

The Draft Recommendations say:

"*…Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes.52…"*

"…Some examples of technical, contractual and organisational measures that could be considered may be found in the non-exhaustive lists described in the Annex 2…"

"…the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them…"

"…the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured…"

"…the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,…"[4]

Our Response

It is our view that the paragraphs above and wider "Step 4" recommendations (including Annex 2) are disproportionate and unrealistic on the part of the EDPB and as a result risk making Article 46 tools unworkable for the vast majority of data exporters.

Dismissal of other alternative supplementary measures

The Draft Recommendations makes it clear that the EDPB considers that contractual and organisational supplementary methods will not be enough and instead focuses heavily on technical measures. Whilst the Court in Case C-311/18 does state that "standard data protection clauses" cannot, by their very nature, bind the public authorities of third countries and that in these cases additional safeguards should be implemented, neither it nor any of the Articles or Recitals to the GDPR specifically refer to the supplementary measures having to be technical ones. In fact Recital 109 to the GDPR refers specifically to other contractual commitments supplementing the standard protection clauses.

Whilst the Draft Recommendations are correct when they state that contractual measures are not generally capable of binding the authorities of a third country when they are not party to the contract, the conclusion that therefore technical measures must also be used does not necessarily follow. It is foreseeable that the assessment at Step 3 of the Draft Recommendations could reveal that a slight strengthening of the standard contractual measures, with for example some of the example clauses in Annex 2 of the Draft Recommendations, would give an essentially equivalent level of protection. The recommendations' general insistence on technical measures being employed should therefore be softened somewhat. Ultimately the solution here must be political rather than commercial.

Practical Issues

The recommendations relating to technical measures, in particular that given in the examples in Annex 2, is not clear enough and has unrealistic expectations. Phrases such as "state of the art" and "robust against cryptanalysis" provide no useful benchmark for data exporters wanting to know if their systems comply. The requirements to also assess the cyber-capabilities of the public authorities of third countries is unrealistic – such capabilities are generally considered state secrets and a part of a country's national security.

[4] Draft Recommendations, pages 15-17 and 21-37

Whilst there may be some technology businesses capable of claiming compliance, for the vast majority of data exporters compliance with "Step 4" of the Draft Recommendations as currently drafted is unclear, unrealistic and unworkable.

The recommendations in the examples given also, save for data protected by legal privilege or medical/professional secrecy, require data to be made non-readable to the data importer. This requirement is incompatible with many current data exporting purposes as it would block the usability of the data by the data importer. Not only would this stop many current inter-business transactions and operations, but it also would severely hinder intra-group operations for international businesses.

In relation to paragraph 52 of the Draft Recommendations, guidance on how quickly one must suspend or end transfers currently occurring would be helpful as currently nothing is stated.

Commercial Impact

Similarly to the points made in our response to Issue 1, the current Draft Recommendations' "Step 4" requirements will cause major commercial impacts upon businesses. For many, were they to try and follow the Draft Recommendations, it would make trade/business, where personal data is transferred, with countries not in the EU or not covered by an adequacy decision become too costly. As mentioned before, the likely effect of this would either be cases of non-compliance with the Draft Recommendations or a reduction in world trade and competition, which would hinder not only most data exporter's interests but also those of their data subjects.

Conclusion For Issue 2

It is our opinion that, given the lack of any such specification in the GDPR or in Case C-311/18, that the Draft Recommendations at Step 4 focus too heavily on technological measures and fails to properly consider alternatives. The Draft Recommendations' current requirements for technological measures are also not clear enough, disproportionate and unrealistic in their expectations of data exporters. The resulting effect of the Draft Recommendations at Step 4 being that it makes Article 46 tools unworkable for the vast majority of data exporters and in turn would likely lead to either non-compliance or a reduction in competition which would harm data subjects more than it would protect their interests.

In our opinion, the Draft Recommendations should instead: consider to a greater extent non-technological measures; where technological measures are recommended, clarify the standards and focus on a proportionate level of technological measures given the risk identified in Step 3; and remove unrealistic expectations that data exporters will be able to investigate the cyber capabilities of third countries. It should also, in the spirit of transparency and pragmatism, recognise that many of the issues it seeks to resolve here are political rather than commercial, and will need a political rather than corporate solution.

Issue 4: Step 6: Re-evaluate at appropriate intervals

Your Draft Recommendation
The Draft Recommendations say: *"You must monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country to which you have transferred personal data that could affect your initial assessment of the level of protection and the decisions you may have taken accordingly on your transfers. Accountability is a continuing obligation (Article 5(2) GDPR)[5]"*
Our Response
Step 6 does not clearly identify what triggers a re-evaluation of the previous steps, but simply states this to be an ongoing and continuing obligation. It is clear that steps 3 and 4, in particular, are not straightforward so this step essentially places onto data exporters an ongoing burden of a process which was not made clear to them in the first place. This would arguably leave data exporters in a place of confusion and uncertainty which is of concern.
Conclusion For Issue 4
Further guidance is required highlighting in what circumstances would a re-evaluation be necessary and how often should this take place as a minimum requirement. Will their obligation reflect that placed on the Commission's adequacy decisions under article 45 where decisions must be reviewed every 4 years?[6] Whatever the case may be, this clarification would arguably ease the concerns of data exporters with regards to this ongoing obligation. Further clarification and guidance is also required with regards to the previous steps.

EMW LAW LLP

UNITED KINGDOM

21 DECEMBER 2020

[5] Draft Recommendations, page 18

[6] Article 45(3) GDPR

We welcome the EDPB's feedback and comments on this consultation and would be willing to engage in further consultation and dialogue if the EDPB feels this would be valuable.

For further communication, please contact:

Matthew Holman
Principal
Head of Technology & Data Protection Law

EMW Law LLP
90 Chancery Lane
London
WC2A 1EU

Telephone: +44 207 405 4440
Email: Matthew.Holman@emwllp.com